

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of
INFORMATION ASSOCIATED WITH
FOREVASTACC1N@ICLOUD.COM THAT IS STORED AT
PREMISES CONTROLLED BY APPLE, INC.

Case No: 4:22 MJ 1191 JMB

FILED UNDER SEALSIGNED AND SUBMITTED TO THE COURT FOR FILING BY
RELIABLE ELECTRONIC MEANS**APPLICATION FOR A SEARCH WARRANT**

I, Michele Steinman, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| <i>Code Section</i> | <i>Offense Description</i> |
|---|---|
| 18 U.S.C. § 1708, § 513(a), § 1344, § 1029 | Theft or Receipt of Stolen Mail Matter, Possession of Counterfeit Securities, Bank Fraud, Fraud and Related Activity in Connection with Access Devices |

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.

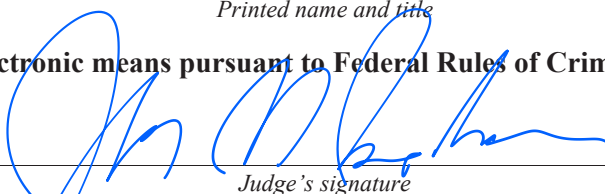


Applicant's signature

Michele Steinman, Postal Inspector, USPIS

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 3 June 2022City and state: St. Louis, MO


Judge's signature

Honorable John M. Bodenhause, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

| | | |
|---------------------------------|---|---------------------------------------|
| IN THE MATTER OF THE SEARCH OF |) | 4:22 MJ 1191 JMB |
| INFORMATION ASSOCIATED WITH |) | |
| FOREVASTACC1N@ICLOUD.COM |) | <u>FILED UNDER SEAL</u> |
| THAT IS STORED AT PREMISES |) | |
| CONTROLLED BY APPLE, INC. |) | SIGNED AND SUBMITTED TO THE COURT FOR |
| |) | FILING BY RELIABLE ELECTRONIC MEANS |

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michele Steinman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am employed as a United States Postal Inspector with the United States Postal Inspection Service and have been so employed since February of 2022. My duties as a Postal Inspector include the investigations of mail theft (18 U.S.C. § 1078), bank fraud (18 U.S.C. §

1344), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), identity theft (18 U.S.C. § 1028) aggravated identity theft (18 U.S.C. § 1028A) and other criminal activities. Prior to becoming a Postal Inspector, I was a Special Agent with the United States Department of Treasury, Internal Revenue Service Criminal Investigation (IRS-CI) for approximately 5 years. Before that, I was employed for 12 years as a Special Agent in the United States Secret Service. In both of these previous federal law enforcement positions, I performed investigations involving violations of state and federal law, including cases involving fraudulent activities.

3. As a result of my training and experience in my current and prior positions, I am familiar with federal criminal laws. My primary duties have been the enforcement of federal laws pertaining to financial fraud, identity theft, tax fraud, cyber-crime and other areas. I have worked on numerous criminal investigations during my federal law enforcement career, often involving fraud, money laundering and other criminal activities, including being the lead investigative agent. During the course of these investigations, I have planned, led, and participated in the execution of search warrants, arrest warrants, witness and suspect interviews, surveillances, assisted during judicial proceedings and other duties.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1708 (Theft or Receipt of Stolen Mail Matter), 18 U.S.C. § 513(a) (Possession of Counterfeit Securities), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1029 (Fraud and Related Activity in Connection with Access Devices), and conspiracy

to commit such offenses, have been committed by DENNIS COOPERWOOD JR. (“COOPERWOOD”) and others, both known and unknown, in this investigation. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

LOCATION TO BE SEARCHED

7. The location to be searched is the Apple account associated with Apple ID **FOREVASTACC1N@ICLOUD.COM** (hereinafter referred to as “**Subject Account**”), located at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, CA 95014.

BACKGROUND CONCERNING APPLE¹

8. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

9. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

10. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email

addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

11. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

12. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

13. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial

number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

14. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

15. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

16. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. For example, geo-location data could show a subjects location at or during the commission of a crime, during the capturing of photos, recording of videos, and message content may provide knowledge of the scheme and participants involved in the burglaries and/or sale of the stolen merchandise. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

17. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

18. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

19. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. These apps may be used to anonymize communications, encrypt communications, advertise stolen goods, ship stolen goods, and accept payment for stolen goods. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

20. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

A. The Fraud Scheme

21. Beginning in approximately August 2021, the United States Postal Inspection Service and the United States Postal Service – Office of Inspector General (collectively,

“investigators”) began receiving reports of personal checks, which victims had placed in USPS collection boxes, being altered and deposited in multiple bank accounts around the St. Louis, MO area. In summary, as part of the investigation, investigators have spoken with victims, who have confirmed their checks had been placed in the U.S. mail and subsequently altered or counterfeited. Investigators have also obtained and reviewed records from the banks into whose accounts these checks were deposited, including surveillance video from ATM machines and bank locations, which depict multiple suspects depositing these altered or counterfeited checks. Bank records also indicate that suspects, before banks learn the deposited check was altered or counterfeit, withdraw or attempt to withdraw, the proceeds of these checks via cash withdrawals or electronic transfers.

22. As part of the investigation, investigators have determined that suspects often use mobile devices, including iPhones, for a variety of purposes in furtherance of the scheme, including the following:

a. to communicate with other participants in the scheme before, during, and after their criminal activities. For instance, investigators have identified multiple social media accounts that appeared to have been used to recruit and communicate with bank account holders to provide their debit card, PIN, and banking information to be used for the deposit of an altered or counterfeit check. Investigators have also identified other forms of electronic communication, such as text messages, voice messages, and video calls, between participants in the scheme.

b. to take pictures and videos to memorialize their criminal activities and the fruits of the scheme. For instance, posts on social media used to recruit bank account holders often include photos and videos depicting debit cards, ATMs, and large amounts of U.S. currency. Suspects have also shared photos and videos of stolen checks, both before and after being altered. These photos and videos are consistent with being made or taken on a smart phone.

B. Arrest of COOPERWOOD

23. On or about April 12, 2022, was arrested by the St. Louis County, MO Police Department during a traffic stop. The following information was provided to investigators by the St. Louis County, MO Police Department.

24. On or about April 12, 2022, officers with the St. Louis County Police Department, on patrol in the area of Garden Drive North and Dunn Road in north St. Louis County, observed a vehicle stopped in the middle of the road on Garden Drive and multiple people standing at the windows of the vehicle. As officers approached in their marked police vehicle, the people around the vehicle quickly dispersed, and the vehicle began to drive towards Dunn Road. As the vehicle drove away, officers observed the license plate light on the vehicle was not properly illuminated. Based on this violation, officers conducted a traffic stop of the vehicle at the intersection of Garden Drive and Dunn Road. As officers approached the vehicle, officers observed three occupants in the vehicle. During the traffic stop, officers identified the rear passenger as COOPERWOOD.

25. During the traffic stop, officers requested to search the occupants and the vehicle, and COOPERWOOD and the other occupants provided consent to search. Officers then removed a shoulder bag in COOPERWOOD's possession and searched the bag. In COOPERWOOD's bag, officers observed multiple checks, none of which had COOPERWOOD's name on them. In some instances, there were multiple checks from same payors. In total, officers counted 179 checks, which varied in payors and dollar amounts.

26. When COOPERWOOD was asked by the officers why he had so many checks and why the checks did not appear to belong to him, COOPERWOOD told officers he bought the checks from unidentified individuals, used a toothpick or etching tool to remove the ink written in pen and then sold the checks to other unidentified individuals.

27. Officers placed COOPERWOOD under arrest for possession of/receiving stolen property based on their knowledge of recent thefts involving checks from area mailboxes and the belief the checks in COOPERWOOD's possession were related to said thefts and the fact that COOPERWOOD had already told officers he participated in the forging and altering of the checks. COOPERWOOD was subsequently transported to the St. Louis County, MO Justice Center.

28. As part of investigation, detectives with the St. Louis County Police Department spoke with victims whose checks were found in COOPERWOOD's possession. Based on these interviews, detectives with the St. Louis County Police Department determined that almost all of the checks in COOPERWOOD's possession were stolen after being placed in USPS mailboxes in the St. Louis area. For example, multiple checks belonged to business victim Flooring Systems Inc. Detectives spoke with the CEO of Flooring Systems Inc., who told detectives he routinely placed his outgoing business mail in blue collection boxes in the St. Louis area to be mailed. Detectives were also told that COOPERWOOD did not work for Flooring Systems Inc. and the only way COOPERWOOD would have possession of the checks was if they had been stolen.

C. Interview of COOPERWOOD

29. On or April 13, 2022, investigators and a detective from St. Louis County, MO Police Department interviewed COOPERWOOD at the St. Louis County, MO Justice Center. At the onset, COOPERWOOD waived his *Miranda* rights and agreed to speak with investigators. COOPERWOOD also signed a St. Louis County Police Department Warning and Waiver form indicating the same.

30. During the interview, COOPERWOOD made the following statements:

a. COOPERWOOD admitted to investigators that he bought and sold checks that did not belong to him. COOPERWOOD further admitted to removing the ink/altering the checks after buying them and then selling the altered checks to unknown persons for a profit.

b. COOPERWOOD stated he became involved in the buying and selling of checks approximately three weeks ago. He had heard from other unnamed individuals “on the street” about the buying/washing/selling of checks. COOPERWOOD admitted to purchasing checks for \$5-\$10 each, then removing the ink and selling the checks with the removed ink for \$20-\$25 each or in sets of 2 or 3. COOPERWOOD denied negotiating or depositing any of the checks himself at any financial institution. When asked if COOPERWOOD knew the checks in his possession were stolen, he acknowledged by stating “yeah probably.” He further acknowledged he knew it was wrong to alter or “wash” checks. COOPERWOOD denied knowing the checks were stolen from the U.S. Mail and also denied knowing about a scheme involving checks stolen from the U.S. Mail that were altered and later deposited. He claimed he did not know what the individuals he sold checks to were doing with the altered checks.

c. COOPERWOOD claimed he was introduced to this scheme to alter checks through a middleman, who he only knew as “Murda.” COOPERWOOD learned through the internet and other individuals how to remove the ink from the checks using brake fluid, a toothpick or a nail.

d. “Murda” arranged the meetings for COOPERWOOD to purchase the checks. COOPERWOOD communicated with “Murda” using the messaging feature on his Apple iPhone. COOPERWOOD denied having cell service and indicated that he used his phone while connected to Wi-Fi to use the Apple iMessage feature to communicate with “Murda.”

COOPERWOOD identified his iCloud account associated with his iPhone as **FOREVASTACC1N@ICLOUD.COM** (the “**Subject Account**”).²

e. COOPERWOOD claimed he bought checks from the same individual on 3 or 4 separate occasions the past few weeks. All of these meetings were set up by “Murda” with COOPERWOOD using his cell phone/iCloud account to communicate. The meetings took place in business parking lots such as Arby’s, Wal-Mart, etc. around the St. Louis area. COOPERWOOD claimed that, on each occasion, he bought the checks from the same unknown, older black male in a black pickup truck, possibly a Ford, after “Murda” set up the meeting for him.

f. After he would purchase the checks, COOPERWOOD indicated that he altered them and removed the ink using the self-taught methods he previously described. He would then sell the checks to other individuals and make a profit. He admitted to selling altered checks to persons unknown three to five times. All of these transactions were again set up by “Murda” using COOPERWOOD’s cell phone. He generally sold checks to the unknown persons in sets of two or three.

g. COOPERWOOD claimed he and “Murda” split the proceeds from the sales of the altered checks, with COOPERWOOD getting 60% and “Murda” receiving 40%.

² During the initial interview on April 13, 2022, investigators initially wrote down the iCloud account provided by COOPERWOOD as “for3vastacc1n@iCloud.com,” however, it was determined that was not a valid account. A follow up phone call was conducted with COOPERWOOD on April 19, 2022, who stated that was not correct and provided the correct spelling of his iCloud account, **forevastacc1n@iCloud.com**.

D. The Subject Account

31. On or about April 19, 2022, a preservation request was sent to Apple, Inc. to preserve the records associated with the **Subject Account**.

32. Investigators requested and received records from Apple regarding the **Subject Account** which showed it was a valid account and data was preserved in the account.

33. As recently as May 6, 2022, investigators have continued to receive reports from victims and local law enforcement agencies within the Eastern District of Missouri regarding the theft of personal and business checks from USPS collection boxes, the altering of those checks, and the depositing of those checks in third party bank accounts.

CONCLUSION

34. Based on the forgoing, I request that the Court issue the proposed search warrant.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



MICHELE STEINMAN
Postal Inspector
United States Postal Inspection Service

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on 3 June, 2022.



HONORABLE JOHN M. BODENHAUSEN
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **FOREVASTACC1N@ICLOUD.COM**, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (“Apple”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 1, 2022 through the date of this warrant, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2022, through the date of this warrant, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1708 (theft or receipt of stolen mail matter), 18 U.S.C. § 513(a) (possession of counterfeit securities), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1029 (fraud and related activity in connection with access devices), involving DENNIS COOPERWOOD JR. and unknown others since January 1, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence of the theft, receipt, and possession of stolen mail matter;
- (b) Evidence of the theft, receipt, and possession of third parties' banking information and other personal identifiable information;
- (c) Evidence of the alteration of checks and possession of altered checks, and the creation, receipt, and possession of counterfeit checks;
- (d) Evidence of the sale of checks or stolen mail matter, and how proceeds from the sale of checks or stolen mail matter were spent, maintained, or distributed;
- (e) Evidence indicating how and when the Apple account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Apple account owner;
- (f) Evidence indicating the Apple account owner's state of mind as it relates to the crime under investigation;
- (g) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS
PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND
902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature